Re.

09/429,624

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/429,624	10/29/99	YUNG M	10624.0015

LM02/1003

STUART T F HUANG
STEPTOE & JOHNSON LLP
1330 CONNECTICUT AVENUE NW
WASHINGTON DC 20036-1795

EXAMINER	
TUCKER, C	
ART UNIT	**PAPER NUMBER**
2766	6

DATE MAILED: 10/03/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

SK

Office Action Summary	Application No.	Applicant(s)	
	09/429,624	YUNG ET AL.	
	Examiner	Art Unit	
	Christopher M. Tucker	2766	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-11 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-11 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a)☐ All b)☐ Some * c)☐ None of the CERTIFIED copies of the priority documents have been:

1.☐ received.

2.☐ received in Application No. (Series Code / Serial Number) _____ .

3.☐ received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. & 119(e).

Attachment(s)

15)☒ Notice of References Cited (PTO-892)
16)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
17)☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5 .
18)☐ Interview Summary (PTO-413) Paper No(s). _____ .
19)☐ Notice of Informal Patent Application (PTO-152)
20)☐ Other: .

DETAILED ACTION

Drawings

1. This application has been filed with informal drawings which are acceptable for examination purposes only. Formal drawings will be required when the application is allowed.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1-11 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-71 of U.S. Patent No. 6,035,041. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following reasons. Claims 1-11 differ from claim 1-71 of '041 in that they recite generating random values using the shared values. However, it would have been obvious to one of ordinary skill in the art at the time of the invention to generate random values from the shared values to increase the difficulty of an intruder guessing the new keys.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

4. Claims 1-10 are rejected under 35 U.S.C. 102(a) as being anticipated by Gennaro et al. (hereinafter, "Gennaro") in *Robust Threshold DSS Signatures.*

5. As per claim 1, Gennaro discloses a method of using distributed cryptographic keys between a plurality of distributed electronic devices, said distributed electronic devices capable of communication with a central server, said method comprising the steps of computing shared values over a known and agreed context, generating random values using said shared values, generating a partial result for each device using said random values, and computing an output based on said partial result (pages 361-368).

6. As per claim 2, Gennaro discloses the method of using distributed cryptographic keys as recited by claim 1, wherein said shared values are random keys (pages 361-368).

7. As per claim 3, Gennaro discloses the method of using distributed cryptographic keys as recited by claim 1, wherein said shared values are derived from a cryptographic protocol (pages 361-368).

8. As per claim 4, Gennaro discloses the method of using distributed cryptographic keys as recited by claim 1, wherein said shared values are derived cryptographically (pages 361-368).

9. As per claim 5, Gennaro discloses the method of using distributed cryptographic keys as recited by claim 1, further comprising the step of implementing a re-representation of a function (pages 361-368).

10. As per claim 6, Gennaro discloses the method of using distributed cryptographic keys as recited by claim 1, wherein said partial results may include incorrect values (page 361-368).

11. As per claim 7, Gennaro discloses the method of using distributed cryptographic keys as recited by claim 1, wherein the steps in claim 1 are performed iteratively (pages 361-368).

12. As per claim 8, Gennaro discloses the method of using distributed cryptographic keys as recited by claim 7, further comprising changing said shared values after said step of generating an output based on said partial result (pages 361-368).

13. As per claim 9, Gennaro discloses the method of using distributed cryptographic keys as recited by claim 3, wherein said cryptographic protocol is a cryptographic function involving exponentiation (pages 361-368).

14. As per claim 10, Gennaro discloses the method of using distributed cryptographic keys as recited by claim 3, wherein said cryptographic protocol is an RSA function (pages 361-368).

15. Claims 1-4 and 9-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Brickell et al. (hereinafter, "Brickell") (U.S. 5,867,578).

16. As per claim 1, Frankel discloses a method of using distributed cryptographic keys between a plurality of distributed electronic devices, said distributed electronic devices capable of communication with a central server, said method comprising the steps of computing shared values over a known and agreed context, generating random values using said shared values, generating a partial result for each device using said random values, and computing an output based on said partial result (column 3, line 66 – column 4, line 20; column 9, line 10 – column 10, line 31; column 11, line 10 – column 12, line 39; columns 20-23).

17. As per claim 2, Brickell discloses the method of using distributed cryptographic keys as

recited by claim 1, wherein said shared values are random keys (column 9, line 10 – column 10, line 31; column 11, line 10 – column 12, line 39).

18. As per claim 3, Brickell discloses the method of using distributed cryptographic keys as recited by claim 1, wherein said shared values are derived from a cryptographic protocol (column 9, line 10 – column 10, line 31; column 11, line 10 – column 12, line 39).

19. As per claim 4, Brickell discloses the method of using distributed cryptographic keys as recited by claim 1, wherein said shared values are derived cryptographically (column 9, line 10 – column 10, line 31; column 11, line 10 – column 12, line 39).

20. As per claim 9, Brickell discloses the method of using distributed cryptographic keys as recited by claim 3, wherein said cryptographic protocol is a cryptographic function involving exponentiation (column 9, line 10 – column 10, line 31).

21. As per claim 10, Brickell discloses the method of using distributed cryptographic keys as recited by claim 3, wherein said cryptographic protocol is an RSA function (column 8, lines 31-47; column 10, lines 52-53).

22. As per claim 11, Brickell discloses the method of using distributed cryptographic keys as recited by claim 1, wherein said shared values are stored in a hardware device in at least one of said distributed devices (column 7, line 49 – column 8, line 14).

Conclusion

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher M. Tucker whose telephone number is 703 306 5539. The examiner can normally be reached on M-F between the hours of 8:30 and 4:30 with alternating Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail O. Hayes can be reached on 703 305 9711. The fax phone numbers for the organization where this application or proceeding is assigned are 703 305 0040 for regular communications and 703 305 0040 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 305 3900.

CMT
CMT
September 30, 2000

Gail Hayes
Gail Hayes
Supervisory Primary Examiner
Art Unit 2766